

EXHIBIT "1"

PETER D. KEISLER
Assistant Attorney General
Civil Division
United States Department of Justice

EUGENE M. THIROLF
Director
Office of Consumer Litigation

ALAN J. PHELPS
D.C. Bar No. 475938
Trial Attorney
Office of Consumer Litigation
United States Department of Justice
1331 Pennsylvania Ave. NW, Suite 950N
Washington, DC 20004
Tel: 202-307-6154
Fax: 202-514-8742
E-mail: alan.phelps@usdoj.gov

Attorneys for the United States

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

HASMIK JASMINE PAPAZIAN,)	No. CV 07-1479 GPS (RZx)
)	
Plaintiff,)	<u>BRIEF OF THE UNITED STATES</u>
)	<u>IN SUPPORT OF 15 U.S.C.</u>
v.)	<u>§ 1681c(g)</u>
)	
BURBERRY LIMITED, et al.,)	
)	
Defendants.)	Honorable George P. Schiavelli
)	
)	

TABLE OF CONTENTS

INTRODUCTION	4
ARGUMENT	4
A. <u>The requirements of § 1681c(q) are clear</u>	5
B. <u>Section 1681c(q) does not violate the First Amendment</u>	7
CONCLUSION	21

TABLE OF AUTHORITIES

<u>44 Liguormart, Inc. v. Rhode Island</u> , 517 U.S. 484 (1996) . . .	8
<u>Aeschbacher v. California Pizza Kitchen</u> , 2007 WL 1500853 (C.D. Cal. Apr. 3, 2007)	7
<u>Arcilla v. Adidas Promotional Retail Operations, Inc.</u> , 488 F. Supp.2d 965, 2007 WL 1498334 (C.D. Cal. May 4, 2007)	7
<u>Big Bear Super Market No.3 v. INS</u> , 913 F.2d 754 (9th Cir. 1990)	6
<u>Bolger v. Youngs Drug Product Corp.</u> , 463 U.S. 60 (1983) . . .	11
<u>California Teachers Ass'n v. Bd. of Educ.</u> , 271 F.3d 1141 (9th Cir. 2001)	6
<u>Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y.</u> , 447 U.S. 557 (1980)	11-13
<u>City of Dallas v. Stanglin</u> , 490 U.S. 19 (1989)	9
<u>Clark v. Cmty. for Creative Non-Violence</u> , 468 U.S. 288, 293 n. 5 (1984)	10
<u>Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.</u> , 472 U.S. 749 (1985)	10
<u>Greater New Orleans Broad. Ass'n v. United States</u> , 527 U.S. 173 (1999)	12, 13
<u>Hill v. Colorado</u> , 530 U.S. 703 (2000)	5
<u>Hurley v. Irish-Am. Gay, Lesbian & Bisexual Group</u> , 515 U.S. 557, 569-70 (1995)	9
<u>Lopez v. Gymboree Corp.</u> , 2007 WL 1690886 (N.D. Cal., June 9, 2007)	7
<u>Lorillard Tobacco v. Reilly</u> , 533 U.S. 525 (2001)	12, 13

1	<u>Pirian v. In-N-Out Burgers</u> , 2007 WL 1040864 (C.D. Cal. Apr. 5,	
2	2007)	7
3	<u>Rumsfeld v. F.A.I.R.</u> , 547 U.S. 47, 126 S.Ct. 1297 (2006) . . .	9
4	<u>Soualian v. Int'l Coffee & Tea LLC</u> , Case No. CV 07-502-RGK (C.D.	
5	Cal., June 11, 2007)	4
6	<u>Spence v. Washington</u> , 418 U.S. 405, 410-11 (1974)	9
7	<u>Spikings v. Cost Plus, Inc.</u> , Case No. CV 06-8125-JFW (C.D. Cal.	
8	May 25, 2007)	4
9	<u>Texas v. Johnson</u> , 491 U.S. 397 (1989)	9
10	<u>Three Affiliated Tribes of Fort Berthold Reservation v. Wold</u>	
11	<u>Engineering, P. C.</u> , 467 U.S. 138 (1984)	4
12	<u>Trans Union v. FTC</u> , 245 F.3d 809 (D.C. Cir. 2001) . . .	8, 12-13
13	<u>Trans Union v. FTC</u> , 267 F.3d 1138 (D.C. Cir. 2001)	8, 20
14	<u>Turner Broad. System, Inc. v. FCC</u> , 520 U.S. 180, 217-18 (1997)	20
15	<u>United Reporting Pub. Corp. v. California Highway Patrol</u> , 146	
16	F.3d 1133 (9th Cir. 1998)	11
17	<u>United States v. Powell</u> , 423 U.S. 87 (1975)	6
18	<u>Universal City Studios, Inc. v. Corely</u> , 273 F.3d 429 (2d Cir.	
19	2001)	8
20	<u>Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.</u> ,	
21	455 U.S. 489 (1982)	6
22	<u>Villegas v. City of Gilroy</u> , 484 F.3d 1136 (9th Cir. 2007) . . .	9
23	<u>Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer</u>	
24	<u>Council, Inc.</u> , 425 U.S. 748 (1976)	8

INTRODUCTION

Pursuant to 28 U.S.C. § 2403, the United States of America ("United States") hereby submits this brief in defense of Section 113 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") (codified at 15 U.S.C. § 1681c(g)) and against the constitutional challenges presented by Defendant Burberry Limited in the Counterclaim included with Defendants' Answer (Dkt. #10). Section 1681c(g) is neither impermissibly vague nor does it infringe on any First Amendment right. The United States respectfully requests that the Court find § 1681c(g) constitutional.

ARGUMENT

As an initial matter, the government understands that Plaintiff's motion for class certification also is pending before this Court. The government does not intervene to take a stand on this issue, but notes that at least two courts in cases exactly like this one ruled against class certification. See Soualian v. Int'l Coffee & Tea LLC, Case No. CV 07-502-RGK (C.D. Cal., June 11, 2007) (available at 2007 U.S. Dist. LEXIS 44208); Spikings v. Cost Plus, Inc., Case No. CV 06-8125-JFW (C.D. Cal. May 25, 2007) (available at 2007 U.S. Dist. LEXIS 44214). Were this Court to also find against class certification, the case likely would be resolved without the necessity of determining the constitutional questions raised by Defendant. Therefore, the Court need not reach the constitutional issues at this time, depending on the outcome of the class certification motion. See Three Affiliated Tribes of Fort Berthold Reservation v. Wold Engineering, P. C., 467 U.S. 138, 157 (1984) ("It is a fundamental rule of judicial

1 restraint . . . that this Court will not reach constitutional
2 questions in advance of the necessity of deciding them.").
3 Should the Court determine that resolution of the constitutional
4 questions is presently necessary, however, case law provides
5 ready answers.

6 **A. The requirements of § 1681c(g) are clear**

7 Section 1681c(g) reads, in relevant part, as follows:

8 (g) Truncation of credit card and debit card numbers.

9
10 (1) In general. Except as otherwise provided
11 in this subsection, no person that accepts
12 credit cards or debit cards for the
13 transaction of business shall print more than
14 the last 5 digits of the card number or the
15 expiration date upon any receipt provided to
16 the cardholder at the point of the sale or
17 transaction.

14 15 U.S.C. § 1681c.

15 Defendant asserts that § 1681c(g) is impermissibly vague
16 because it does not specify whether retailers must truncate card
17 numbers *and also* delete expiration dates. Defendant claims that
18 the statute can reasonably be read to allow printing of a card
19 expiration date so long as the card number itself is truncated.
20 Such a reading ignores the plain language and purpose of the
21 provision. The statute as written does not offend due process
22 concerns.

23 A statute is unconstitutionally vague only if (1) "it fails
24 to provide people of ordinary intelligence a reasonable
25 opportunity to understand what conduct it prohibits" or (2) "it
26 authorizes or encourages arbitrary and discriminatory
27 enforcement." Hill v. Colorado, 530 U.S. 703, 732 (2000). This
28 requirement of a "reasonable" degree of clarity does not mean

1 Congress must use the most precise language conceivable. "The
2 fact that Congress might, without difficulty, have chosen clearer
3 and more precise language equally capable of achieving the end
4 which it sought does not mean that the statute which it in fact
5 drafted is unconstitutionally vague." United States v. Powell,
6 423 U.S. 87, 94 (1975) (quotation omitted).

7 Furthermore, as the Supreme Court has emphasized, "economic
8 regulation is subject to a less strict vagueness test [than
9 criminal statutes] because its subject matter is often more
10 narrow, and because businesses, which face economic demands to
11 plan behavior carefully, can be expected to consult relevant
12 legislation in advance of action." Village of Hoffman Estates v.
13 Flipside, Hoffman Estates, Inc., 455 U.S. 489, 498 (1982)
14 (footnote omitted); see also Big Bear Super Market No. 3 v. INS,
15 913 F.2d 754, 757 (9th Cir. 1990) ("when the statute regulates
16 the conduct of businesses . . . the vagueness test is relaxed,
17 because businesses have a greater ability to determine the
18 meaning of legislation in advance of their conduct than do
19 individuals.").

20 Vagueness concerns are more acute where a statute implicates
21 First Amendment rights. See Hoffman Estates, 455 U.S. at 499.
22 As set out below, the statute at issue does not restrict actual
23 speech protected by the First Amendment. Even if § 1681c(g)
24 applied to true expression, however, "perfect clarity is not
25 required even when a law regulates protected speech." California
26 Teachers Ass'n v. Bd. of Educ., 271 F.3d 1141, 1150 (9th Cir.
27 2001) (citing Ward v. Rock Against Racism, 491 U.S. 781, 794
28 (1989)). "[E]ven when a law implicates First Amendment rights,

1 the constitution must tolerate a certain amount of vagueness."
2 Id. at 1151.

3 Section 1681c(g) easily passes muster under either vagueness
4 test because no reasonable person would read the statute in any
5 way other than prohibiting the printing on receipts of both
6 expiration dates and full card numbers. Read in the unreasonable
7 manner Defendant suggests, § 1681c(g) would allow retailers to
8 print full credit/debit card numbers so long as they did not
9 print the expiration date. Def.'s Mem. in Opp'n. to Pl.'s Mot.
10 to Dismiss, Dkt. # 21 ("Def.'s Br.") at 4. Congress could not
11 have intended that absurd result. Indeed, at least four courts
12 have recently found, in the context of motions to dismiss brought
13 in cases mirroring the present action, that § 1681c(g) clearly
14 prohibits printing expiration dates. See Lopez v. Gymboree
15 Corp., 2007 WL 1690886, *3 (N.D. Cal., June 9, 2007); Arcilla v.
16 Adidas Promotional Retail Operations, Inc., 488 F. Supp.2d 965,
17 2007 WL 1498334, *3-5 (C.D. Cal. May 4, 2007); Pirian v. In-N-Out
18 Burgers, 2007 WL 1040864, *3 (C.D. Cal. Apr. 5, 2007);
19 Aeschbacher v. California Pizza Kitchen, 2007 WL 1500853, *3
20 (C.D. Cal. Apr. 3, 2007). Those courts were correct; the
21 argument advanced by Defendant has no merit.

22 **B. Section 1681c(g) does not violate the First Amendment**

23 Defendant's First Amendment claim is similarly unconvincing.
24 First, it is highly questionable whether Defendant's procedure of
25 copying card expiration dates and numbers to cash register
26 receipts constitutes speech at all. Second, even if the act of
27 transferring expiration dates to paper involves expressive
28

1 speech, the government's restriction on that speech is extremely
2 limited, reasonable, and constitutional.

3 Accepting a credit/debit card from a customer, copying the
4 card number or expiration date onto a receipt, and immediately
5 handing the card with receipt back to the customer is a rote act
6 devoid of expression and not "speech" covered by the First
7 Amendment. Defendant attempts to liken printing expiration dates
8 to commercial advertisements, instructions, or computer code.
9 Def.'s Br. at 8-9. While it is true that dry facts in
10 advertisements or instructions such as computer code can
11 constitute speech, that is not the situation here. All of the
12 cases Defendant cites involve statements laden with actual
13 information flowing from one party to another. See 44
14 Liquormart, Inc. v. Rhode Island, 517 U.S. 484 (1996) (liquor
15 store advertisements); Virginia State Bd. of Pharmacy v. Virginia
16 Citizens Consumer Council, Inc., 425 U.S. 748 (1976) (pharmacy
17 drug prices); Universal City Studios, Inc. v. Corely, 273 F.3d
18 429 (2d Cir. 2001) (computer code). Defendant's actions involve
19 no such expression of information; rather, the "speech" at issue
20 is more akin to the act of putting a credit card on a photocopy
21 machine and pressing the button.¹ The fact that Defendant's
22 conduct results in a printed date does not, by itself, implicate
23 the First Amendment. "[I]t has never been deemed an abridgment
24

25 ¹ As discussed below, courts have applied commercial speech
26 analysis in the context of other FCRA provisions. See Trans
27 Union v. FTC, 245 F.3d 809 (D.C. Cir. 2001); Trans Union v. FTC,
28 267 F.3d 1138 (D.C. Cir. 2001). In these cases, however, the
communications at issue involved far more than simply copying a
date from a card to a piece of paper. Rather, these cases
concerned the sale of mailing lists containing contact
information for consumers who met specific criteria.

1 of freedom of speech or press to make a course of conduct illegal
2 merely because the conduct was in part initiated, evidenced, or
3 carried out by means of language, either spoken, written, or
4 printed." Rumsfeld v. Forum for Academic and Institutional
5 Rights, Inc., 547 U.S. 47, 126 S.Ct. 1297, 1308 (2006) (quotation
6 omitted).

7 Conduct can constitute speech, but only if it involves
8 expression. For good reason, not all conduct qualifies for First
9 Amendment protection. "It is possible to find some kernel of
10 expression in almost every activity a person undertakes - for
11 example, walking down the street, or meeting one's friends at a
12 shopping mall - but such a kernel is not sufficient to bring the
13 activity within the protection of the First Amendment." City of
14 Dallas v. Stanglin, 490 U.S. 19, 25-26 (1989) (law imposing age
15 limits on dance halls did not violate First Amendment freedom of
16 association). Communicative, constitutionally protected conduct
17 requires an intent to convey a particularized message that is
18 likely to be understood by those viewing it. See Spence v.
19 Washington, 418 U.S. 405, 410-11 (1974) (flying flag upside down
20 found expressive); see also Hurley v. Irish-Am. Gay, Lesbian &
21 Bisexual Group, 515 U.S. 557, 569-70 (1995) (discussing instances
22 in which the Supreme Court has found conduct to be inherently
23 communicative); Texas v. Johnson, 491 U.S. 397, 404 (1989)
24 (burning of flag found expressive); Villegas v. City of Gilroy,
25 484 F.3d 1136, 1139-41 (9th Cir. 2007) (wearing of vests with
26 skull insignia signifying no particular message found not
27 expressive). Furthermore, it is the duty of the party seeking to
28 engage in allegedly expressive conduct to demonstrate that the

1 First Amendment applies to that conduct. Clark v. Cmty. for
2 Creative Non-Violence, 468 U.S. 288, 293 n. 5 (1984) ("Although
3 it is common to place the burden upon the Government to justify
4 impingements on First Amendment interests, it is the obligation
5 of the person desiring to engage in assertedly expressive conduct
6 to demonstrate that the First Amendment even applies.").
7 Defendant offers no plausible argument that copying a date
8 already in the possession of a customer from one place to another
9 is an inherently expressive activity. It fact, such an action
10 communicates nothing in particular.

11 Even if Defendant could make a case that copying a date from
12 plastic to paper constitutes actual expressive speech, it would
13 be considered, at best, commercial speech. See Trans Union v.
14 FTC, 295 F.3d 42, 52-53 (D.C. Cir. 2002) (upholding a different
15 section of the FCRA and analyzing it under the commercial speech
16 doctrine). The Supreme Court has "long recognized that not all
17 speech is of equal First Amendment importance. It is speech on
18 matters of public concern that is at the heart of the First
19 Amendment's protection." Dun & Bradstreet, Inc. v. Greenmoss
20 Builders, Inc., 472 U.S. 749, 758-59 (1985) (quotations omitted).
21 In particular, "[commercial speech] may be regulated in ways that
22 might be impermissible in the realm of noncommercial expression."
23 Id. at 759 n.5 (citations omitted).

24 Defendant contends that because expiration dates are not
25 advertisements and do not refer to specific products, they cannot
26 be considered commercial speech. Def.'s Br. at 7, n.4.
27 Therefore, Defendant claims, printing expiration dates on
28 receipts actually deserves greater First Amendment scrutiny than

1 advertisements. Id. Defendant relies for this proposition on
2 the discussion of commercial speech in Bolger v. Youngs Drug
3 Product Corp., 463 U.S. 60 (1983), which found that such speech
4 often constitutes advertising in some form, references a
5 particular product, and is motivated by economic considerations.
6 Bolger, 463 U.S. 67-68.

7 Contrary to Defendant's argument, commercial speech is not
8 limited to advertisements for specific products, under Bolger or
9 any other case. As the Ninth Circuit has held, whether something
10 constitutes advertising "is the beginning of our inquiry . . .
11 not the end." United Reporting Pub. Corp. v. California Highway
12 Patrol, 146 F.3d 1133, 1137 (9th Cir. 1998) (rev'd. on other
13 grounds, Los Angeles Police Dept. v. United Reporting Pub. Corp.,
14 528 U.S. 32 (1999)). The Bolger Court itself explicitly stated
15 that commercial speech does not require "each of the
16 characteristics present in this case." Bolger, 463 U.S. at 67
17 n.14. In the seminal Central Hudson case, decided just a few
18 years prior to Bolger, the Supreme Court noted that commercial
19 speech can include any "expression related solely to the economic
20 interests of the speaker and its audience." Central Hudson Gas &
21 Electric Corp. v. Public Service Comm'n of New York, 447 U.S.
22 557, 561 (1980).

23 The Central Hudson definition is far more broad than the one
24 Defendant attempts to impose through its misreading of Bolger.
25 It covers the "speech" at issue, which, even as Defendant
26 describes it, does nothing more than confirm details of a
27 private, commercial transaction. See Def.'s Answer and
28 Counterclaim (Dkt. #10) ¶ 40 (printing of expiration date meant

1 to "confirm to [Defendant's] customers that a transaction has
2 been appropriately charged."). Such a communication relates only
3 to the economic interests of the merchant and the consumer. It
4 does not touch on any matter of public concern. It constitutes,
5 if anything, commercial speech.

6 Under Central Hudson's intermediate scrutiny test, the Court
7 must examine whether 1) the speech concerns lawful activity and
8 is not misleading; 2) the asserted government interest is
9 substantial; 3) the regulation directly serves that interest; and
10 4) the regulation is no more extensive than necessary to serve
11 that interest. Central Hudson, 447 U.S. at 566. Elaborating on
12 the last factor, the Supreme Court has made clear that "[t]he
13 Government is not required to employ the least restrictive means
14 conceivable, but it must demonstrate narrow tailoring of the
15 challenged regulation to the asserted interest - 'a fit that is
16 not necessarily perfect, but reasonable; that represents not
17 necessarily the single best disposition but one whose scope is in
18 proportion to the interest served.'" Greater New Orleans Broad.
19 Ass'n v. United States, 527 U.S. 173, 188 (1999) (quoting Board
20 of Trustees of State Univ. of N. Y. v. Fox, 492 U.S. 469, 480
21 (1989)); Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 556
22 (2001) (explicitly stating that case law does not require "the
23 least restrictive means," but only a "reasonable fit."); see also
24 Trans Union v. FTC, 245 F.3d 809, 818-19 (D.C. Cir. 2001)
25 ("Because the FCRA is not subject to strict First Amendment
26 scrutiny . . . Congress had no obligation to choose the least
27 restrictive means of accomplishing its goal."). Furthermore,
28 while the commercial speech test requires more than "mere

1 speculation or conjecture" that the restriction advances the
2 government interest, Greater New Orleans, supra, at 188, neither
3 does it require "a surfeit of background information." Lorillard
4 Tobacco, 533 U.S. at 555. The means used to achieve a
5 permissible goal can be justified "solely on history, consensus,
6 and 'simple common sense.'" Id. (quoting Florida Bar v. Went For
7 It, Inc., 515 U.S. 618, 628 (1995)).

8 The facts of this case meet the first prong of the Central
9 Hudson test, in that copying expiration dates is not misleading
10 and concerns otherwise lawful transactions. Regarding the second
11 prong, Defendant does not, and can not, deny the government's
12 significant interest in preventing identity theft. See Def.
13 Answer at ¶ 42 ("Congressional concern about identity theft was
14 valid."); Trans Union, 245 F.3d at 818 (governmental interest in
15 "protecting the privacy of consumer credit information . . . is
16 substantial."). The dispute, therefore, centers on the third and
17 fourth prongs of Central Hudson, and specifically Defendant's
18 assertion that the combination of an expiration date and a
19 truncated card number cannot possibly be used to facilitate the
20 type of fraud Congress wanted to prevent.

21 Congress sought with FACTA to "assist[] consumers in
22 preventing identity theft and for mitigating its consequences
23 once the crime has occurred." See 108 H. Rep. No. 263 (2003).
24 The goal of the provision that became § 1681c(g) was to "limit
25 the opportunities for identity thieves to 'pick off' key card
26 account information." S. Rep. No. 108-166 (2003). FACTA
27 followed enactment of laws in at least 20 states with provisions
28 similar to § 1681c(g) that prohibited printing the full card

1 number as well as the expiration date on receipts.² A handful of
 2 other states passed laws focused only on the card number.³ As
 3 shown by the final language of § 1681c(g), Congress mandated the
 4 more comprehensive version of these restrictions as the national
 5 standard. Congress' decision to protect both card numbers and
 6 expiration dates from inadvertent disclosure through discarded
 7 sales receipts, as many states had already done, directly serves
 8 the interest Congress sought to protect through the least
 9 restrictive means available.

10 Defendant claims that expiration dates accompanied only by
 11 truncated card numbers need no protection from would-be
 12 fraudsters. Defendant submitted with its opposition to
 13 Plaintiff's motion the declaration of a former MasterCard
 14 employee who stated that a full expiration date and a truncated
 15 card number cannot be used to make fraudulent transactions.
 16 Decl. of Joel Lisker, Dkt. #22. Defendant also contends, based
 17

18 ² See Ariz. Rev. Stat. Ann. § 44-1367 (2001); Ark. Code
 19 Ann. § 4-107-303 (West 2003); Cal. Civ. Code § 1747.09 (West
 20 2007); Colo. Rev. Stat. Ann. § 6-1-711 (West 2006); Conn. Gen.
 21 Stat. Ann. § 42-133hh (West 2003); Fla. Stat. Ann. § 501.0188
 22 (West 2003); Ga. Code Ann. § 10-15-3 (2007); Idaho Code Ann.
 23 § 28-51-103 (2003); 815 Ill. Comp. Stat. Ann. 505/2mm (West
 24 2004); Kan. Stat. Ann. § 50-669b (2002); La. Rev. Stat. Ann.
 25 § 9:3518.3 (2001); Me. Rev. Stat. Ann. Tit. 10, § 1149 (2004);
 Nev. Rev. Stat. Ann. § 597.945 (West 2003); N.J. Stat. Ann.
 § 56:11-42 (West 2002); N.Y. Gen. Bus. Law § 520-a (McKinney
 2003); N.D. Cent. Code § 51-07-27; Ohio Rev. Code Ann. § 1348.18
 (West 2002); Okla. Stat. Ann. Tit. 15, § 752a (West 2002); Tex.
 Bus. & Com. Code Ann. § 35.61 (Vernon 2003); Utah Code Ann.
 § 13-38-101 (West 2003); Va. Code Ann. § 11-33.2 (West 2004);
 Wash. Rev. Code Ann. § 19.200.010 (West 2000).

26 ³ See Del. Code Ann. Tit. 11, § 915a (2003); Md. Code Ann.,
 Commercial Law § 14-1318 (West 2003); Mo. Ann. Stat. § 407-433
 27 (West 2003); Neb. Rev. Stat. § 28-633 (2002); N.m. Stat. Ann.
 § 56-4-3.1 (West 2003); N.c. Gen. Stat. Ann. § 14-113.24 (West
 28 2003); Or. Rev. Stat. Ann. § 646.888 (West 2007); Wis. Stat. Ann.
 § 134.74 (West 2002).

1 on the same declaration, that card companies routinely complete
2 transactions with incorrect expiration dates so long as the
3 expiration date provided to the merchant is in the future.
4 Def.'s Br. at 3. Therefore, Defendant claims, a restriction on
5 copying expiration dates to sales slips does not advance the
6 government's interest in preventing identity theft and other
7 fraud.

8 Defendant's argument that a thief would not be able to make
9 fraudulent charges using only a truncated card number and the
10 full expiration date misses the point. Thieves might piece
11 together (or "pick off," in the words of Congress) different bits
12 of information from different sources. The expiration date of a
13 customer's credit/debit card, until recently printed on
14 Defendant's receipts, is one of several pieces of information
15 that can make it easier for criminals to rack up fraudulent
16 charges. These dates are worth protecting even when not
17 accompanied by other important financial information.⁴

18 Congress' actions comport with common experience, testimony
19 provided in support of the legislation, and the instructions
20

21 ⁴ Mr. Lisker also opines that an identity thief who
22 obtained information such as a victim's Social Security number
23 could open accounts under the victim's name and make fraudulent
24 charges to those new accounts. Expiration dates of existing,
25 legitimate cards may not be pertinent to someone creating new,
26 fraudulent accounts from scratch. However, the constitutionality
27 of § 1681c(g) does not require that the provision help fight all
28 types of fraud.

25 Mr. Lisker further argues that consumers suffer little or no
26 damage from unauthorized use of their credit cards because of
27 laws and policies limiting their liability. Even if victims
28 themselves rarely incur any direct monetary loss due to credit
card fraud, such losses are paid by consumers everywhere in the
form of higher bank fees or in the costs for goods and services.
Consumer victims also spend valuable time reporting and otherwise
dealing with this type of fraud.

1 credit card companies give to merchants. For instance, Mari J.
2 Frank, author of a declaration cited in Mr. Lisker's declaration,
3 testified to Congress that expiration dates should be eliminated
4 from sales receipts. On May 15, 2003, Ms. Frank advocated for a
5 rule stating that "[n]o company or entity shall print more than
6 the last 5 digits of a credit card number or account number or
7 the expiration date upon any receipt provided to a cardholder."
8 See Testimony of Mari J. Frank, May 15, 2003, before the House
9 Gov't. Reform Comm. (available at 2003 WL 21130287) (emphasis
10 added). Ms. Frank was not alone in pressing Congress to protect
11 expiration dates. Michael D. Cunningham, Senior Vice President
12 of Credit and Fraud Operations for Chase Cardmember Services,
13 testified before the Senate Banking Committee in 2003 that much
14 of the fraud his company encountered occurred when a card
15 "account number and expiration date is compromised[,] permitting
16 purchases by phone, mail, or Internet." See S. Hrg. 108-579,
17 June 19, 2003, before the Senate Comm. on Banking, Housing, and
18 Urban Affairs. Linda Foley, Executive Director of the Identity
19 Theft Resource Center, recommended that Congress require
20 businesses to print only truncated card numbers and no expiration
21 dates on receipts. Id.

22 Anyone who has used a credit or debit card for telephone or
23 online transactions knows that retailers, especially those
24 accepting orders over the phone or through the Internet, require
25 expiration dates to complete transactions. That common
26 experience is borne out by the policies of credit card companies.
27 For example, VISA publishes a handout for merchants entitled "If
28

1 the Card is NOT There - You Need to be MORE Aware." That
2 document instructs merchants to:

3 Ask the customer for the card expiration date and
4 include it in your authorization request. An invalid
5 or missing expiration date can be an indicator that the
person on the other end does not have the actual card
in hand.

6 Ex. A.⁵ In another publication called "Rules for VISA
7 Merchants," VISA again states, in a section entitled "Fraud
8 Prevention Guidelines for Card-Not-Present Transactions," that
9 businesses should:

10 Whenever possible, . . . ask customers for their card
11 expiration, or "Good Thru," date and include it in
12 [the] authorization requests. Including the date helps
13 to verify that the card and transaction are legitimate.
A [mail order/telephone order] or Internet order
containing an invalid or missing expiration date may
indicate counterfeit or unauthorized use.

14 Ex. B (excerpts from VISA Rules) at 32 (emphasis added).⁶ Those
15 same Rules further state:

16 Key-entered transactions are fully acceptable, but they
17 are associated with higher fraud and chargebacks rates.
18 In addition, when transactions are key-entered, the
19 benefits associated with special security features -
20 such as the expiration date and Card Verification Value
2 (CVV2) - are not available.

21 Rules, p. 31 (emphasis added).⁷

22 ⁵ Available at
http://usa.visa.com/download/merchants/card_not_there_aware.pdf.

23 ⁶ Available at
24 [http://usa.visa.com/download/merchants/rules_for_visa_merchants.p](http://usa.visa.com/download/merchants/rules_for_visa_merchants.pdf)
df.

25 ⁷ In her declaration, Ms. Frank quotes another section of
26 the "Rules for Merchants" document for the proposition that all
27 expiration dates are automatically considered correct in
28 telephone, mail, or Internet transactions. See Frank Decl. (Dkt.
#22, Ex. B) at 5. However, the page from which Ms. Frank quotes
deals with chargeback "Code 73: Expired Card" and specifies that
"[m]any Merchant Banks automatically handle this type of
chargeback, so you never really see it." Id. at 103. A

1 Other credit card companies similarly advise merchants to
 2 verify expiration dates as a way of helping to prevent fraud.
 3 Ms. Frank's declaration quotes a "financial crimes expert" with
 4 American Express as stating that "60% of the time the expiration
 5 date is not evaluated for verification purposes." Frank Decl.
 6 (Dkt. #22, Ex. B) at 14. In other words, according to the
 7 documents submitted by Defendant, the expiration date is
 8 evaluated for verification purposes in almost half of American
 9 Express transactions. The "Fraud Prevention Handbook," provided
 10 to merchants by American Express, verifies that merchants should
 11 obtain the expiration date, especially for "card-not-present"
 12 transactions:

13 When you are accepting an American Express Card for
 14 mail, telephone or Internet transactions, obtain the
 Cardmember's:

- 15 1. Name exactly as it appears on the Card
- 16 2. Card account number
- 17 3. Expiration date on the Card (valid date) . . .

18 Call American Express Authorizations . . . to verify
 19 the billing address and CID. Address verification must
 be done for charges when merchandise will be shipped.
 Provide:

- 20 - Cardmember account number
- 21 - Expiration date

22
 23
 24 _____
 25 chargeback occurs when a transaction is reversed and cancelled.
 This section of the "Rules" does not support the broad conclusion
 Ms. Frank draws from it.

26 Furthermore, as stated elsewhere in its Rules for Merchants,
 27 VISA does consider expiration dates to be one way to help verify
 legitimate transactions. The statements of VISA's Joseph Majka,
 28 as related in Ms. Frank's declaration, do not address the issue
 of whether expiration dates are sometimes used to help verify
 transactions as legitimate. See Frank Decl. at 8.

1 Ex. C (Excerpts from American Express "Handbook") at 38.⁸
2 American Express also urges merchants not to print expiration
3 dates on receipts in order to protect that information against
4 fraud:

5 As an American Express merchant, you are responsible
6 for helping to ensure that your customer's credit card
7 information is secured and protected against future
8 fraud activity. Here are a few steps that you can take
9 to protect this information:

10 . . . Do not print the Card expiration date or your merchant
11 account number on the terminal (customer) receipt. Only
12 print a "subset" of the Card account numbers on the terminal
13 (customer) receipt.

14 Id. at 39 (emphasis added).

15 The company that manages the Discover Card also requests
16 that merchants obtain expiration dates when processing online or
17 over-the-phone orders. See Ex. D at 41.⁹ In an online document
18 entitled "Fraud Prevention/Card Not Present," Discover explains
19 to merchants that the "Types of Suspicious Behavior" potentially
20 indicative of fraud includes when a "[c]ustomer instructs you to
21 try different expiration dates when initial attempts fail." Ex.
22 E (emphasis added) at 44.¹⁰

23 As illustrated by these instructions from credit card
24 companies to merchants, expiration dates should be used to
25 evaluate the legitimacy of transactions. If a customer provides

26 ⁸ Available at
27 [https://www209.americanexpress.com/merchant/singlevoice/resources](https://www209.americanexpress.com/merchant/singlevoice/resources/FPHANDcvr.pdf)
28 [/FPHANDcvr.pdf](https://www209.americanexpress.com/merchant/singlevoice/resources/FPHANDcvr.pdf).

⁹ Available at
http://www.discovernetwork.com/home/data/fraud_faq.html.

¹⁰ Available at
[http://www.discovernetwork.com/resources/data/card_not_present.ht](http://www.discovernetwork.com/resources/data/card_not_present.html)
[ml](http://www.discovernetwork.com/resources/data/card_not_present.html).

1 an expiration date that does not match the true date, the
2 authorization may fail. Expiration dates may not be examined in
3 every case; the thoroughness of the verification process is
4 determined to a large extent by individual merchants, their
5 banks, and the customer's card issuer. But expiration dates
6 plainly are not extraneous information, as Defendant suggests.
7 Checking expiration dates and protecting them from casual
8 disclosure is one method that credit card companies, banks, and
9 merchants employ to prevent fraud. See Decl. of Don Coker
10 (submitted with Pl.'s Reply to Def.'s Opp'n. to Pl.'s Mot. to
11 Dismiss Counterclaim) at ¶ 14 (purchase declined at online
12 retailer due to invalid expiration date). Even if that does not
13 happen in every single case, intermediate scrutiny does not
14 obligate courts to invalidate a "remedial scheme because some
15 alternative solution is marginally less intrusive on a speaker's
16 First Amendment interests." Turner Broad. System, Inc. v. FCC,
17 520 U.S. 180, 217-18 (1997) (citations omitted). "So long as the
18 means chosen are not substantially broader than necessary to
19 achieve the government's interest, . . . [a] regulation [is] not
20 . . . invalid simply because a court concludes that the
21 government's interest could be adequately served by some
22 less-speech-restrictive alternative." Id. at 218 (quotation
23 omitted).

24 Here, Congress reasonably determined that expiration dates
25 should be protected, and that conclusion led directly to the
26 extremely limited restriction on the "speech" embodied by
27 § 1681c(g). "[T]he government cannot promote its interest
28 (protection of personal financial data) except by regulating

1 speech because the speech itself (dissemination of financial
2 data) causes the very harm the government seeks to prevent."
3 Trans Union v. FTC, 267 F.3d 1138, 1141 (D.C. Cir. 2001). The
4 restriction, in other words, directly serves the government's
5 interest by means no more restrictive than necessary. In fact,
6 the prohibition affects no other speech whatsoever, either
7 indirectly or unintentionally. It does not even prevent
8 Defendant from doing what it claims to do by printing such
9 information: Customers can confirm that transactions were
10 properly charged by looking at the truncated card number and
11 other information on the receipt, without the expiration date.
12 In any calculation of the costs and benefits of § 1681c(g), the
13 "cost" column would have to be set at zero. It easily passes the
14 Central Hudson test.

15 CONCLUSION

16 Section 1681c(g) directly advances the government's
17 legitimate interest in preventing identity theft and related
18 fraud by means that are as narrowly tailored as possible.
19 Furthermore, the terms of the statute are clear. The United

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

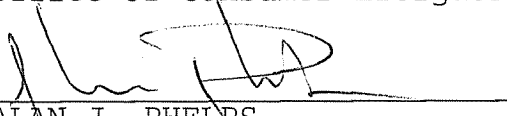
1 States asks that this Court find the provision constitutional, if
2 it determines that it must reach the constitutional question at
3 all.

4
5 Respectfully submitted,

6 PETER D. KEISLER
7 Assistant Attorney General
8 Civil Division
9 United States Department of Justice

10 EUGENE M. THIROLF
11 Director
12 Office of Consumer Litigation

13 Dated: July 24, 2007


14 ALAN J. PHELPS
15 Office of Consumer Litigation
16 U.S. Department of Justice
17 1331 Penn. Ave. NW Suite 950N
18 Washington, DC 20004

19 Attorneys for the United States
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Brief of the United States in Support of 15 U.S.C. § 1681c(g) was sent via electronic mail and facsimile this 24th day of July, 2007, to the following:

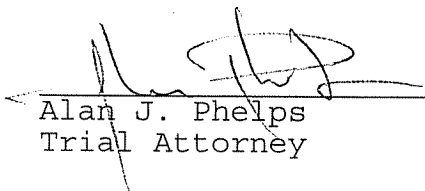
Camille E. Bennett
Harold C. Hirshman
Sonnenschein Nath & Rosenthal
7800 Sears Tower
Chicago, IL 60606
fax: (312) 876-7934

David H. Stern
Sonnenschein Nath & Rosenthal
601 S. Figueroa St., Ste. 1500
Los Angeles, CA 90017-5704
fax: (213) 623-9924

Attorneys for Defendants

Launa Nicole Everman
Wayne S. Kreger
Milstein Adelman and Kreger
2800 Donald Douglas Loop North
Santa Monica, CA 90405
fax: (310) 396-9635

Attorneys for Plaintiff



Alan J. Phelps
Trial Attorney

Exhibit A



With the proper know-how and the right tools, mail order, telephone and Internet merchants can detect fraud and avoid associated card losses.

If the Card is NOT There — You Need to be MORE Aware

To stay ahead of the crooks and reduce your fraud exposure:

- 1 Ask the customer** for the card expiration date and include it in your authorization request. An invalid or missing expiration date can be an indicator that the person on the other end does not have the actual card in hand.
- 2 Use fraud detection** tools like the Address Verification Service (AVS) and Card Verification Value 2 (CVV2) as part of the authorization process. To order the Merchant Guide to AVS (VRM 01.01.06) or the Merchant Guide to CVV2 (VRM 03.14.06) call 1-800-VISA-311 or visit www.visa.com/merchant.
- 3 Be on the lookout** for questionable transaction data or other signs indicating “out of pattern” orders.

If you suspect fraud:

- **Ask the customer** for day/evening phone numbers, then call the customer with any questions.
- **Ask for additional information** (e.g., bank name on the front of card).
- **Separately confirm the order** by sending a note via the customer’s billing address, rather than the “ship to” address.

Report suspicious activity to your merchant bank.



Exhibit B



Rules for Visa Merchants

Card Acceptance and Chargeback Management Guidelines





VisaNet® is part of Visa's consumer payment system. It is itself a collection of systems that includes:

- **An authorization service** through which issuers can approve or decline individual Visa card transactions.
- **A clearing and settlement service** that processes transactions electronically between merchant banks and issuers to ensure that:
 - Visa transaction information moves from merchant banks to issuers for posting to cardholders' accounts.
 - Payment for Visa transactions moves from issuers to merchant banks to be credited to the merchant's account.

Transaction Life Cycles

The following illustrations show the life cycle for Visa card transactions, for both card-present and card-not-present purchases. Processing events and activities may vary slightly for any one merchant, merchant bank, or card issuer, depending on card and transaction type, and the processing system used.

Authorization

1. Cardholder presents a Visa card to pay for purchases. For card-not-present transactions, the cardholder provides the merchant with the account number, expiration date, billing address, and CVV2.

2. Merchant swipes the card, enters the dollar amount, and transmits an authorization request to the merchant bank. For card-not-present transactions, the account number and other information may be digitally or key-entered.

3. Merchant bank electronically sends the authorization request to VisaNet.

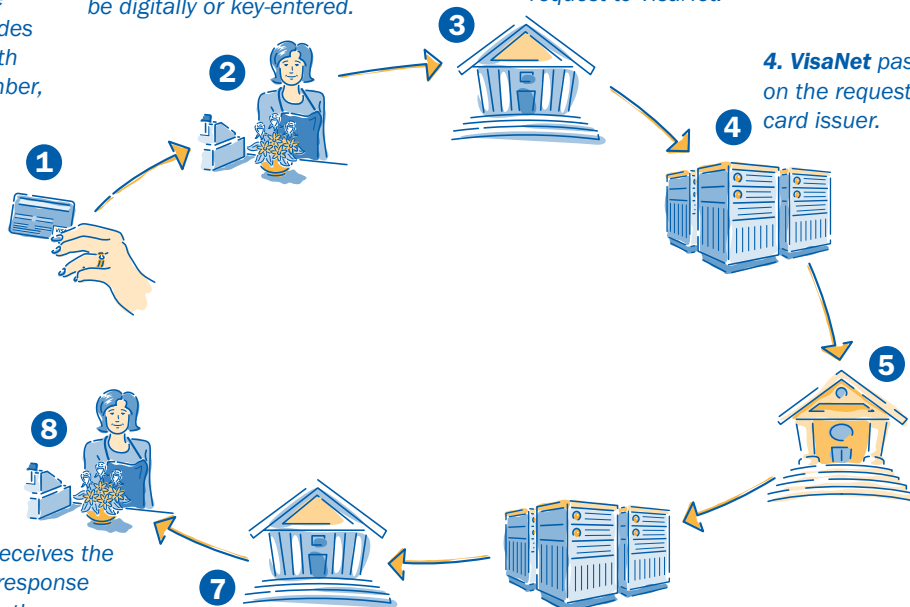
4. VisaNet passes on the request to the card issuer.

5. Card issuer approves or declines the transaction.

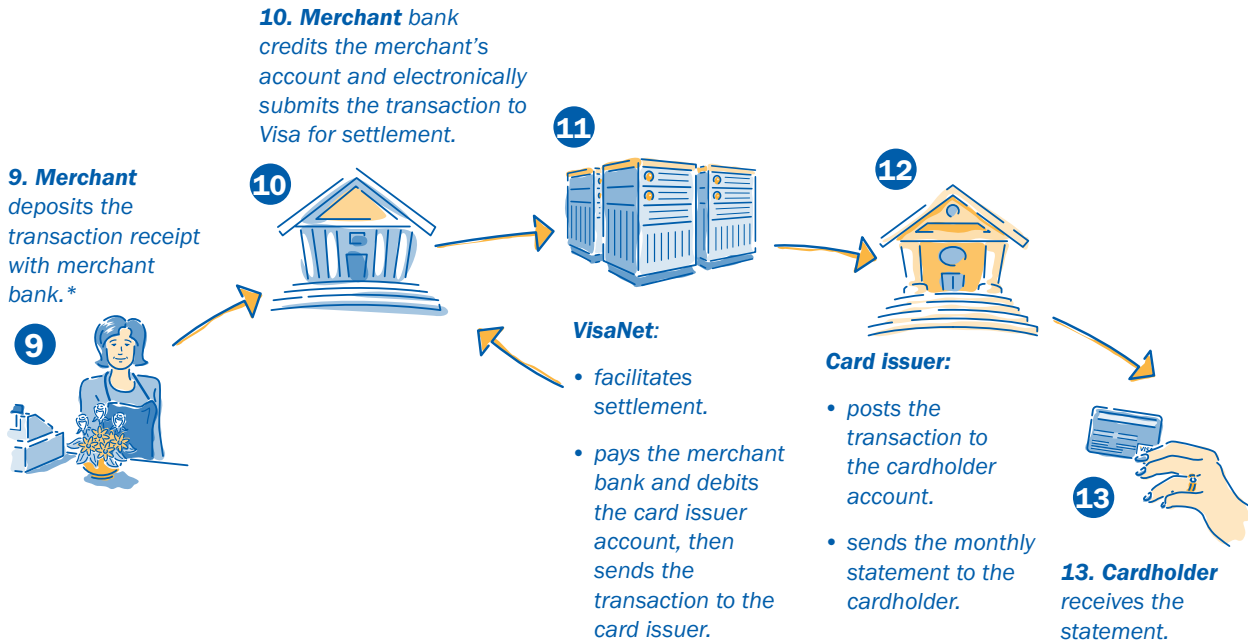
6. VisaNet forwards the card issuer's authorization response to the merchant bank.

7. Merchant bank forwards the response to the merchant.

8. Merchant receives the authorization response and completes the transaction accordingly.



Clearing and Settlement



*Merchants or their agents that store, process, or transmit data may not store sensitive authentication data (full magnetic-stripe or chip) contents. Card Verification Value 2 (CVV2), or PIN Verification Value (PVV)—even if it is encrypted. Once an authorization is processed, such data should no longer exist. The only components of the magnetic stripe that can be stored are name, account number, and expiration date.

DCC Transaction Receipt Requirements

For both a card-present or card-not-present environment, a DCC transaction must contain all of the following:

- Transaction amount of the goods or services purchased in the merchant's local currency—including currency symbol next to the amount
- Exchange rate, including any commission
- Total price in the transaction currency, accompanied by the words "Transaction Currency"—including currency symbol next to the amount
- A disclaimer that:
 - is easily visible to the cardholder,
 - specifies that the cardholder has been offered a choice of payment in the merchant's local currency, and that the cardholder understands the choice of currency is final

Fashion Store Location Date and Time	
Merchant ID	xxxxx
Terminal ID	xxxxx
Date:	Time:
Invoice No:	Auth No:
VISA	SALE
Card No	xxxxxxxxxxxx6330
Exp. Date	xx/xx
Sale Amount	100 Merchant Currency
Tax	2
Total Amount	102 Merchant Currency
Exchange Rate:	
+ Commission: xx.xx	
Sale Amount	\$ 65 Transaction Currency
I accept that I have been offered a choice of currencies for payment & that this choice is final.	
Signature: _____	

Truncated Account Number

Visa requires that all new electronic POS terminals provide account number truncation on transaction receipts. This means that only the last four digits of an account number should be printed on the customer's copy of the receipt.

After July 1, 2006, the expiration date should not appear at all. Existing POS terminals must comply with these requirements by July 1, 2006. To ensure your POS terminals are properly set up for account number truncation, contact your merchant bank.



Key-entered transactions are fully acceptable, but they are associated with higher fraud and chargebacks rates. In addition, when transactions are key-entered, the benefits associated with special security features—such as the expiration date and Card Verification Value 2 (CVV2)—are not available.

How to Minimize Key-Entered Transactions

These best practices can help you keep key-entered transactions at acceptably low levels and should be incorporated into your daily operations and staff training and review sessions.

Pinpoint Areas with High Key-Entry Rates

Calculate the percentage of key-entered transactions compared to total transactions to pinpoint which stores, terminals, or sales associates have high key-entry rates. Merchants are encouraged to monitor their key-entry rates on a monthly basis.

To obtain the percentage of key-entered transactions for a particular terminal, divide the total number of key-entered transactions by the total number of sales. Exclude from both totals any mail or telephone orders that may have been made at the terminal. Perform the above calculation for each terminal, and for each sales shift to determine the key-entry rate per sales associate. Repeat the process for each store, as appropriate.

Find Causes and Look for Solutions

If your key-entry rates are greater than one percent per terminal or sales associate, you should investigate the situation and try to find out why. The following chart summarizes the most common reasons for high key-entry rates and provides possible solutions.

KEY-ENTRY CAUSE	SOLUTION
Damaged Magnetic-Stripe Readers	Check magnetic-stripe readers regularly to make sure they are working.
Dirty Magnetic-Stripe Readers	Clean magnetic-stripe reader heads several times a year to ensure continued good use.
Magnetic-Stripe Reader Obstructions	Remove obstructions near the magnetic-stripe reader. Electric cords or other equipment could prevent a card from being swiped straight through the reader in one easy movement.
Spilled Food or Drink	Remove any food or beverages near the magnetic-stripe reader. Falling crumbs or an unexpected spill could soil or damage the machines.
Anti-Theft Devices that Damage Magnetic Stripes	Keep magnetic anti-theft deactivation devices away from any counter area where customers might place their cards. These devices can erase a card's magnetic stripe.
Improper Card Swiping	<ul style="list-style-type: none"> • Swipe the card once in one direction, using a quick, smooth motion. • Never swipe a card back and forth. • Never swipe a card at an angle; this may cause a faulty reading.

Fraud Prevention Guidelines for Card-Not-Present Transactions

Visa has established a range of fraud-prevention policies, guidelines, and services for card-not-present merchants. Using these tools will help protect your business from fraud-related chargebacks and losses. MO/TO and Internet merchants should strongly consider developing in-house fraud control policies and providing appropriate training for their employees.

The following sections outline basic fraud-prevention guidelines and best practices for card-not-present merchants.

Authorize All Card-Not-Present Transactions

Authorization is required on **all** card-not-present transactions. Card-not-present transactions are considered as zero-floor-limit sales. Authorization should occur before any merchandise is shipped or service performed.

Ask for Card Expiration Date

Whenever possible, card-not-present merchants should ask customers for their card expiration, or “Good Thru,” date and include it in their authorization requests.

Including the date helps to verify that the card and transaction are legitimate. A MO/TO or Internet order containing an invalid or missing expiration date may indicate counterfeit or other unauthorized use.

Ask for CVV2

The Card Verification Value 2 (CVV2) is a three-digit security number printed on the back of Visa cards to help validate that a customer is in possession of a legitimate card at the time of an order. (See *Visa Card Features and Security Elements* on page 23.)

Studies show that merchants who include CVV2 validation in their authorization procedures for card-not-present transactions can reduce their fraud-related chargebacks.

CVV2 Processing

To ensure proper CVV2 processing for card-not-present transactions, merchants should:

- ✓ Ask card-not-present customers for the last three numbers in or beside the signature panel on the back of their Visa cards.

Section 7:

Chargeback Reason Codes

The chargebacks discussed in this section are grouped into six classifications:

- ✓ Non-Receipt of Information
- ✓ Fraud Codes
- ✓ Authorization Errors
- ✓ Processing Errors
- ✓ Cancelled or Returned
- ✓ Non-Receipt of Goods or Services

Reason Code 73: Expired Card

Definition	The card issuer received a transaction that was completed with an expired card and was not authorized.
Most Common Causes	The merchant accepted a card after its expiration or "Good Thru" date and did not obtain an authorization approval from the card issuer.
Merchant Actions	<p>Back-Office Staff</p> <p>Card Not Expired—Key-Entered Transaction (PR) For key-entered transactions, the expiration date should be on the manually imprinted copy of the front of the card. If the expiration date on sales receipt shows the card had not expired at the time of the sale, send a copy of the receipt to your merchant bank. The chargeback is invalid regardless of whether authorization was obtained.</p> <p>Card Expired, Authorization Obtained (PR) If the card was swiped or a manual imprint made, an authorization approval was obtained as required, inform your bank of the transaction date and amount. Many merchant banks automatically handle this type of chargeback so you never see it.</p> <p>Card Expired, No Authorization Obtained (NR) If the card is expired and you did not obtain an authorization, accept the chargeback.</p> <p>Point-of-Sale Staff</p> <p>Check Expiration Date (PM) Check the expiration or "Good Thru" date on all cards. A card is valid through the last day of the month shown; for example, if the Good Thru date is 04/08, the card is valid through April 30, 2008 and expires on May 1, 2008.</p> <p>Card-Not-Present, Authorization Obtained (PR) If the transaction was a MO/TO or Internet transaction, then the expiration date provided by the cardholder is considered correct. Many merchant banks automatically handle this type of chargeback, so you really never see it.</p>

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 73: Expired Card (continued)

Always Get Authorization Approval for Expired Cards

(PM) Always request an authorization for transactions on expired cards and submit the expiration date on the card as part of the authorization request. The expiration date is submitted automatically when you swipe a card. If a transaction is not approved, do not complete the sale.

Owner/Manager

Check Card Expiration Date

(PM) Periodically remind point-of-sale staff to check the card's expiration date before completing transactions and to always obtain an authorization approval if the card is expired.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Exhibit C



American Express

Fraud Prevention Handbook



Cards

Mail Order, Telephone Order, Internet Order Acceptance Procedures

Since mail, telephone and Internet orders are more susceptible to Card fraud, American Express has designed procedures to help protect the Cardmember and the Service Establishment. By following these procedures, you may prevent a criminal from obtaining merchandise or services at your expense.

When you are accepting an American Express Card for mail, telephone or Internet transactions, obtain the Cardmember's:

1. Name exactly as it appears on the Card
2. Card account number
3. Expiration date on the Card (valid date)
4. Card Identification (CID) number (if your establishment is certified to verify the Card Identification Number)

The CID is a 4-digit number printed above the account number on the face of all American Express Cards. The Card Identification number can help you control fraud:

- The Customer must have the actual Card; carbons and old receipts do not display this number.
 - The CID has the advantages of a personal identification number without the problems. Cardmembers don't have to remember a special code; it's printed on the Card.
 - Fraud associated with stolen Card numbers is greatly reduced as the CID changes each time a new card is issued.
5. Billing address, and the address where the merchandise is to be shipped, (if different from the billing address)

Automatic Address Verification (AAV)

In our on-going commitment to help eliminate fraud in the phone and mail order industry, American Express offers Automatic Address Verification (AAV) for American Express transactions. This system electronically transmits your customer's address and zip code to our Cardmember's file. You receive a code indicating a complete, partial, or no-match for each transaction to help you make informed shipping decisions. AAV is free to merchants and qualified third-party processors. For additional information regarding AAV, contact your American Express Account Representative.

6. Billing address phone number and home or business number
7. Phone number where the Cardmember can be reached (if different from the home or business phone)



Mail Order, Telephone Order, Internet Order Acceptance Procedures (continued)

Additionally:

- If you submit electronically, your electronic Charge Record should indicate "Mail Order," "Phone Order" or "Internet" on the Cardmember billing statement.
- Select shippers that do not allow shipment re-routes.
- If phone/Internet orders are allowed to be picked up at retail locations, require the Card to be presented.

Authorization Procedures

Call American Express Authorizations at (1-800-528-2121) to verify the billing address and CID. Address verification must be done for charges when merchandise will be shipped. Provide:

- Cardmember account number
- Expiration date
- Name as it appears on the Card
- Cardmember billing address
- Card Identification Number

You will be told "yes" or "no" depending on whether or not the billing address and CID match our files. **Remember that the billing address verification and the CID verification are checks, not guarantees that the charge is legitimate.**



The risk of fraud is greater during transactions where the card is not present. Therefore it is important to follow proper security procedures.

Mail Order, Telephone Order, Internet Order Acceptance Procedures (continued)

Reducing Fraud and Chargeback Risk

When the billing address is confirmed but delivery will be to a different address, you help reduce the risk of fraud and chargebacks if you:

- Call back the Cardmember to validate the order. Be sure not to call the phone number received with the order; check the telephone directory, if possible.
- Another way to help control future fraud and chargeback losses is to suppress printing the Card number on the shipping invoice. Instead, you may wish to block out all but the last 4 or 5 digits of the 15-digit Card number (see example – Information Protection, p.9). Additionally, never print the CID number on the shipping invoice.
- Be wary of situations where someone places a telephone order, then sends someone (who does not present the Card) to pick up the merchandise.
- Do not accept a fax of the Card as a valid presentation.
- If transactions are done via the Internet, ensure that sites are secured for electronic commerce with the main emphasis of protecting unauthorized access to the customer card information (e.g., behind a firewall). Transactions should be conducted using browser software that supports industry-standard encryption protocols. Passwords to Merchant Web sites should be changed regularly and never set to default.



As Internet orders become more commonplace, it is important that your procedures include a thorough check of each customer.

Reminders:

- If you fulfill an order more than 30 days after the original authorization, call again for a new approval code before mailing the merchandise.
- Charges cannot be submitted for payment until the merchandise is shipped.

Information Protection/Data Security

As an American Express merchant, you are responsible for helping to ensure that your customer's credit card information is secured and protected against future fraud activity. Here are a few steps that you can take to protect this information:

1. Customer's credit card information should be kept confidential. Any electronically stored Cardmember information should be encrypted and/or password protected. (Consult your Terminal Provider or local software specialty store for assistance.)
2. Store your daily credit card receipts in a secured area and limit access to this information to personnel that need this information for accounting and customer service purposes only.
3. Credit card information that is discarded should be shredded or destroyed. Always destroy unneeded carbon copies of charge forms, lodging portfolios or car rental agreements to prevent misuse of valuable Cardmember information.
4. Do not print the Card expiration date or your merchant account number on the terminal (customer) receipt. Only print a "subset" of the Card account numbers on the terminal (customer) receipt.
5. Only your terminal provider or Helpdesk Representative should make changes or upgrades to your Point of Sale equipment and transmission lines.
6. Monitor behavior and activities of employees, especially in transactions where the Card is out of the customer's possession. Ensure that portable and hand held card reading/capturing devices are not being used by employees to capture card data. Be wary of a "contact person" that shows up regularly to meet with an employee to drop off/pick up a scanner, or to pay off an employee for data that has been collected.

Merchant Name
Street Address
City State Zip Code
Telephone Number

Purchase \$ 53.46

C F FR05T
American E * XXXXXXXXXXXX1008
Auth # 236743
05/25/00 1p:51 Re # 0010013750

Signature: _____
C F FR05T

I AGREE TO PAY ABOVE TOTAL AMOUNT
ACCORDING TO CARD ISSUER AGREEMENT

Only print a "subset" of the Card
account number on the receipt.

Exhibit D



[Register to Use Discovernetwork.com](#)

▶ [About Us](#)
[Help & FAQs](#)

[General FAQs](#)
[Reporting FAQs](#)
[Submission Error Fees FAQs](#)
[Internet FAQs](#)
[Rules and Regulations](#)
[Fraud Prevention](#)
[Fraud Prevention FAQs](#)
[System Requirements](#)
[Account Activation](#)
[Gift Card FAQs](#)
[Online Advertising FAQs](#)
[Automatic Payments FAQs](#)

[Privacy](#)

▶ [Contact Us](#)
[Site Map](#)
[Terms of Use](#)
[Discover Network Acceptance Mark - Guidelines and Logos](#)

Help Topics

Fraud Prevention - Ask The Expert (FAQs)

1. [How can I prevent fraud?](#)
2. [How can I prevent Internet, Mail-Order \(MO\) and Telephone-Order \(TO\) fraud?](#)
3. [Why should I require CID on my Web site?](#)
4. [Why should I require a signature when delivering mail or telephone orders?](#)
5. [Why is data security so important and how can I protect my business and customers from hacking attacks?](#)
6. [Where can I report suspected Merchant Fraud?](#)
7. [Where can I meet other Merchants that may have the same Card Not Present \(CNP\) fraud concerns that I have?](#)
8. [What are some signs of suspicious behavior?](#)
9. [What do I do if I suspect a Card is fraudulent in a Card Present situation?](#)
10. [What are some tools offered by Discover Network to help prevent fraud?](#)

1. How can I prevent fraud?

There isn't a single simple solution or tool to preventing fraud. It takes an assortment of many tools to prevent fraud. The best protection comes from knowledge and understanding of the latest tools and trends impacting the marketplace. Discover Network offers its Merchants numerous tools to assist in the fight against fraud. Reading through the FAQs listed below will help you determine what your business needs to do to reduce your fraud risk. Awareness is the first step towards fighting fraud!

2. How can I prevent Internet, Mail-Order (MO) and Telephone-Order (TO) fraud?

Here are some guidelines for preventing Internet and MO/TO fraud:

Request Cardholders for the following information during the order taking process:

- Cardmember Name, exactly how their name appears on their Discover® Network-issued card
- Card Account Number is at least 16 digits
- Card Expiration Date, four-digit number MM/YY
- [CID \(Card Identification Data\)](#), the three-digit number located on the back of the card in the signature panel
- Card billing address along with the ship-to address (when necessary)
- Home, business or other telephone number where the Cardmember can be reached

For each transaction, be sure to:

- Request and validate the [Card Identification Data \(CID\)](#) (the three-digit code on the back of the card in the signature panel). The CID can be submitted in the electronic authorization request or can be used when calling our authorization center
- Verify the customer's billing address, either electronically or by our automated

Exhibit E



- ▶ [Merchant Resources](#)
- ▶ [Home](#)
- ▶ [Order Signage & Supplies](#)
- ▶ [Fraud Prevention](#)
- ▶ [Card Present](#)
- ▶ [Card Not Present](#)
- ▶ [Discover Network](#)
- ▶ [Security Features](#)
- ▶ [Internet and Protecting](#)
- ▶ [Customer Information](#)
- ▶ [Internet Fraud Alert](#)
- ▶ [Abbreviated Numbers](#)
- ▶ [Fraud Prevention Supplies](#)
- ▶ [Ask the Expert \(FAQs\)](#)
- ▶ [Data Security](#)
- ▶ [Discover Network Gift](#)
- ▶ [Card Products](#)
- ▶ [Payroll Cards](#)
- ▶ [Contactless Payments](#)
- ▶ [Biometrics](#)
- ▶ [Merchant Offers](#)
- ▶ [Online Advertising](#)
- ▶ [Automatic Payments](#)
- ▶ [Change Your Bank](#)
- ▶ [Account Information](#)
- ▶ [Rules and Regulations](#)
- ▶ [Activate Your](#)
- ▶ [Terminal / POS Device](#)
- ▶ [Transaction Processors](#)

Fraud Prevention

Card Not Present

In any situation where a card is not present and you are unable to complete a face-to-face transaction, the opportunity for fraud increases.

Card Not Present (CNP) transactions have become the foundation for commerce over the Internet in addition to mail order and telephone order businesses. To assist your company in reducing fraud exposure, these helpful tips have been developed for Discover® Network Merchants who are doing business in a CNP environment.

- [Authorization Center](#)
- [Helpful Hints to Reduce Chargebacks and Risks](#)
- [Types of Suspicious Behavior](#)

Authorization Center

To obtain an authorization or address verification, or to question the validity of a Discover® Network Issued Credit Card, please call **1-800-347-1111**.

Helpful Hints to Reduce Chargebacks and Risks

- Request and validate the [Card Identification Data](#) (CID) (the three-digit code on the back of the card in the signature panel). The CID can be submitted in the electronic authorization request or can be used when calling our authorization center
- Verify the customer's billing address, either electronically or by our automated phone system (Address Verification System - AVS)
- Check your delivery service contract for who is responsible for merchandise not delivered
- Get a signature for each delivery
- Keep all delivery records
- All declines are final. Do not force through any sales for which you have received any declined response to your authorization request
- If the sale is on a credit card, do not refund in cash or by check. Refund sales on the same card account that the purchase was made on
- Include your common DBA and customer service number on the Cardholder's transaction statement
- Clearly communicate any and all delivery charges, restocking or other fees
- Clearly explain any return policies and offer documentation of this policy with each sale
- When working on a chargeback, document efforts to satisfy the customer
- Respond to all Chargebacks, even the small ones (remember, this is your customer)
- Duplicate charges, or installment plans, unless otherwise stated, require an authorization for each sale

Types of Suspicious Behavior

Please consider that these are only indicators of higher risk transactions. One behavior

alone may not be a concern.

- New customer attempts to make a very large credit card transaction
- Customer doesn't know the [Card Identification Data](#) (CID) found on the back of the Card, indicating that they don't have the actual Card
- Customer's address does not match when attaining an Address Verification
- Shipping to an address other than the billing address
- Customer asks that you try lower dollar amounts when a decline message is received
- Customer instructs you to try different expiration dates when initial attempts fail
- Customer hesitates, or has a long pause, when asked for personal information
- Customer repeatedly sends e-mail messages requesting confirmation of shipment
- Customer attempts to place multiple orders to the same address
- Customer attempts to purchase large quantities of a single item
- Customer purchases several large-ticket items, which do not go together, e.g., appear random
- Customer calls a few minutes before closing and wants several large-ticket items
- Customer requests that sales be split up to avoid paying "import taxes" and/or "duty fees"
- Customer requests shipment to an overseas destination
- Customer seems overly concerned about delivery time frames to overseas destinations
- Customer attempts to place a large order using several credit cards to obtain the total authorization amount
- Customer offers the phone number to an authorization center to speed up the credit card approval process
- Customer has little regard for price
- Customer shows little or no concern for return policies, manufacturer warranties and/or rebates when purchasing in large quantities

*Please refer to your Discover Network [Merchant Operating Regulations](#) for further Card Not Present (CNP) requirements with respect to the submission of sales.

If there is a breach in your system, notify Discover® Network Security within 48 hours at 1-800-347-3083.

Click [here](#) to learn more about our Data Security guidelines and our DISC program.

For more extensive information on fraud prevention, including identifying the Discover Card brand, handling suspicious situations, and recovering lost or stolen cards, please consult your Discover Network [Merchant Operating Regulations](#).

In our efforts to assist our Merchants that conduct e-commerce transactions, Discover Network is a proud sponsor of the Merchant Risk Council. [Learn more](#).

[Fraud Prevention Supplies](#)

[Back to Top](#) 

[Register](#) [About Us](#) [Terms of Use](#) [Privacy](#) [Help & FAQs](#) [Contact Us](#) [Site Map](#)

© 2007 DFS Services LLC